XVI. Science Data Systems

SPACE SCIENCES DIVISION

N67-29157

A. Near-Maximal-Length Cycles With Linear Feedback Shift Registers, *M. Perlman*

1. Introduction

The behavior of synchronously operated shift registers with linear logic feedback has been studied in detail (e.g., Ref. 1). An r-stage linear feedback shift register (FSR) can be used to realize cycle lengths of $2^r - 1$, which are termed maximal. The simplest of these, in terms of the complexity of the feedback logic, are those with two-tap feedback which satisfy the linear recurrence relationship

$$a_n = a_{n-i} \oplus a_{n-r} \tag{1}$$

The subscript n in Eq. (1) refers to the clock pulse time. The bit being fed back at time n is a_n, the modulo 2 sum (i.e., EXCLUSIVE-OR) of the contents of the ith and rth stages at time n. The initial state of the ith stage is a_{-i} where $n = 0$.

Unfortunately, there are many values of r for which maximal-length cycles cannot be realized with two feedback taps (see Ref. 2). In these cases, four or a higher even number of taps are required. As the number of feedback taps increases, the complexity of the feedback function grows sharply. The question then arises: Are near-maximal-length cycles realizable with linear FSRs having feedback functions less complicated than a four-input modulo 2 summer? It will be shown that cycle lengths of $2^s - 2$ and $2^s - 4$ can be realized with s-stage linear FSRs. The feedback functions are (with few exceptions) effectively a three-input modulo 2 summer.

2. Generalized r-Stage FSR With Linear Feedback

In Fig. 1, the stages of the register are designated (left to right) $S_1, S_2, \cdots, S_r$. The output of stage S_i is connected to the input of the modulo 2 summer when $C_{r-i} = 1$. C_0 is always 1, otherwise fewer than r stages would be in use. The external input e is a Boolean constant.

Let x_i represent the present state and X_i the next state of stage S_i. The next state of each stage may be expressed as a linear Boolean function of the present state of one or more stages.

$$
\left.\begin{aligned}
X_1 &= C_{r-1}x_1 \oplus C_{r-2}x_2 \oplus \cdots \oplus C_1 x_{r-1} \oplus x_r \oplus e\\
X_2 &= x_1\\
X_3 &= x_2\\
&\cdot\\
&\cdot\\
&\cdot\\
X_r &= x_{r-1}
\end{aligned}\right\} \qquad (2)
$$

This may be expressed as

$$
\begin{bmatrix} X_1 \\ X_2 \\ \cdot \\ \cdot \\ \cdot \\ X_r \end{bmatrix} = \begin{bmatrix} C_{r-1} & C_{r-2} & \cdots & 1 & 0 \\ 1 & 0 & \cdots & C_1 & 1 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_r \end{bmatrix} \oplus \begin{bmatrix} e \\ \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix} \qquad (3)
$$

or

$$
\mathbf{X} = T\mathbf{x} \oplus \mathbf{L} \qquad (4)
$$

Rules of modulo 2 arithmetic are used in determining $\mathbf{X}$. The $r \times r$ Boolean matrix T is nonsingular since its row (column) vectors are linearly independent (Ref. 3). It is termed an *associated matrix*. T represents the linear transformation of an r component vector (present state of the register) into another r component vector (next state of the register). $\mathbf{L}$ represents a translation. When nonzero (i.e., $e = 1$), the modulo 2 sum of the column vector $\mathbf{L}$ and $T\mathbf{x}$ represents the complementation of the bit being fed back. A linear transformation T followed by a translation is called an affine transformation (Ref. 3). Every translation is one-to-one and has an inverse, and the linear transformation T is one-to-one and has an inverse. Hence, the affine transformation $T\mathbf{x} \oplus \mathbf{L}$ is one-to-one and has an inverse. This is another way of saying that each state has a unique predecessor (or equivalently, distinct states have distinct successors).

Of primary interest are the feedback combinations that yield the longest possible cycle length.

CASE I:

$$
e = 0
$$

Therefore,

$$
\mathbf{L} = 0
$$

and

$$
\mathbf{X} = T\mathbf{x}
$$

This case has been thoroughly analyzed (see Refs. 1 and 4) and is summarized here. The smallest value of k for which $T^k = I$ is the length of the longest possible cycle.

The divisibility properties of $\phi(\lambda)$, the characteristic polynomial of T, and k are related as follows:

The smallest value of k for which

$$
\phi(\lambda) \mid \lambda^k - 1 \qquad (5)
$$

is the length of the longest cycle which always contains the state $00 \cdots 01$. In general,

$$
\phi(\lambda) = |T - \lambda I| = \lambda_r + C_{r-1}\lambda^{r-1} + \cdots + C_1\lambda + 1 \qquad (6)
$$

For simplicity, $+$ is used to represent modulo 2 addition. Also, -1 appears as $+1$ since $-1 \equiv 1 \bmod 2$. In accordance with the Caley–Hamilton theorem (Ref. 3),

$$
\phi(T) = T^k - I = 0
$$

and

$$
T^k = I
$$

Thus, if $\phi(\lambda)$ divides $\lambda^k - 1$ [i.e., $\phi(\lambda)$ is a factor of $\lambda^k - 1$], T satisfies $\lambda^k - 1$ and $T^k = I$. The polynomial of the lowest degree which is satisfied by a square matrix A is the minimal polynomial $m(\lambda)$ of A, and it is unique. Fortunately, as will be shown, $\phi(\lambda) = m(\lambda)$ for the *associated matrix* T.

When $\phi(\lambda)$ is irreducible, the smallest k for which (5) holds is termed the exponent to which $\phi(\lambda)$ belongs. To obtain the longest possible cycle length of an r-stage FSR, one must find an irreducible $\phi(\lambda)$ of degree r which belongs to a maximum exponent. The maximum cycle length is

$$
k = 2^r - 1
$$

The exponent of an irreducible polynomial of degree r which is not maximum divides $2^r - 1$. For every positive integer r, there are $[\varphi(2^r - 1)]/r$ polynomials of degree r that belong to a maximum exponent of $2^r - 1$. The Euler phi-function $\varphi(n)$ is the number of positive integers no greater than the integer n that are relatively prime to n.

Irreducibility is a necessary, but not sufficient, condition for $\phi(\lambda)$ to belong to a maximum exponent. A $\phi(\lambda)$ of degree r that belongs to a maximum exponent characterizes an r-stage maximal length FSR.

Cycle lengths for irreducible polynomials through degree 19 are given in Ref. 5. Irreducible polynomials of degree $r > 1$ will always have an odd number of terms, otherwise $\phi(\lambda)$ will contain $\lambda + 1$ as a factor. Irreducible trinomials of maximum exponent characterize maximal length FSRs with the simplest feedback logic; namely, a two-input modulo 2 summer. As previously stated, trinomials are not always among the $[\varphi(2^r - 1)]/r$ irreducible polynomials of maximum exponent. A conjecture,[1] which has since been proven true, states that every trinomial of degree 8 m ($m = 1,2, \cdots$) is reducible. This is a sufficient, but not necessary, condition for a trinomial to be reducible.

For *repeated* irreducible factors such as $\phi(\lambda) = [g(\lambda)]^{\mu}$,

$$k_\phi = e(\nu)k_g$$

where $e(\nu) = 2^i$ and i is an integer such that $1 \leq (2^i/\nu) < 2$.

Tabulated below are values of $e(\nu)$ for ν from 1 through 10.

ν	$e(\nu)$	ν	$e(\nu)$
1	1	6	8
2	2	7	8
3	4	8	8
4	4	9	16
5	8	10	16

In general, for

$$\phi(\lambda) = [g_1(\lambda)]^{\mu_1} [g_2(\lambda)]^{\mu_2} \cdots [g_m(\lambda)]^{\mu_m}$$

where $g_1(\lambda), g_2(\lambda), \cdots, g_m(\lambda)$ are irreducible,

$$k_\phi = LCM\left[e(\nu_1)\, k_{g_1}, e(\nu_2)\, k_{g_2}, \cdots, e(\nu_m)\, k_{g_m}\right]$$

where LCM denotes the least common multiple.

CASE II:

$$e = 1$$

Then

$$\mathbf{L} = \begin{bmatrix} 1 \\ 0 \\ \cdot \\ \cdot \\ 0 \end{bmatrix}$$

and

$$\mathbf{X} = T\mathbf{x} \oplus \mathbf{L}$$

The transformation T and the translation $\mathbf{L}$ may be combined by bordering T with $\mathbf{L}$ to the right as a column, below with r *zeros*, and below and to the right by a single entry *one* (Ref. 3). The matrix equation (Eq. 3) can thus be written as

$$\begin{bmatrix} X_1 \\ X_2 \\ \cdot \\ \cdot \\ \cdot \\ X_r \\ \hline 1 \end{bmatrix} = \left[\begin{array}{cccccc|c} C_{r-1} & C_{r-2} & \cdots & & C_1 & 1 & 1 \\ 1 & 0 & \cdots & & 0 & 0 & 0 \\ \cdot & \cdot & \cdots & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdots & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdots & & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & & 1 & 0 & 0 \\ \hline 0 & 0 & \cdots & & 0 & 0 & 1 \end{array}\right] \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_r \\ \hline 1 \end{bmatrix} \tag{7}$$

The present state $\mathbf{x}$ is bordered with a *one* to make it conformal with the bordered T matrix and to perform the necessary complementation (i.e., translation) in the feedback to S_1 in Fig. 1. The next state vector $\mathbf{X}$ is also bordered just as $\mathbf{x}$. The *one* in the last row appears for each successive transformation. The matrix

$$\mathbf{A} = \begin{bmatrix} T & \mathbf{L} \\ 0 & 1 \end{bmatrix} \tag{8}$$

[1]Made by S. W. Golomb, formerly of JPL Section 331.

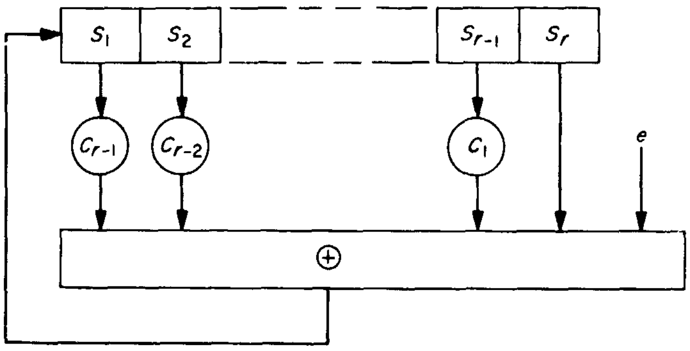

Fig. 1. Generalized r-stage FSR with linear feedback

is of the order $r+1$ by $r+1$ and includes the translation **L**. The characteristic polynomial of A is

$$\theta(\lambda) = \begin{vmatrix} T-\lambda I & \mathbf{L} \\ 0 & 1-\lambda \end{vmatrix} \tag{9}$$

$$\theta(\lambda) = (\lambda + 1)\,\phi(\lambda) \tag{10}$$

where $\phi(\lambda)$ is the characteristic polynomial of T. Just as T, A is nonsingular for all combinations of values of C_i, where $1 \leq i < r$ and $C_0 = 1$. It will be shown that $\theta(\lambda)$ is minimal for A, just as $\phi(\lambda) = m(\lambda)$ for T. Note that the $\lambda + 1$ in Eq. (10) accounts for the complementation of the bit being fed back. The degree of $\phi(\lambda)$ determines the number of stages required. When the feedback of an FSR characterized by $\phi(\lambda)$ is complemented, it will be designated by $\phi(\lambda)^*$ where $\phi(\lambda)^* = [\theta(\lambda)]/(\lambda + 1)$.

3. The Minimal Polynomial of the T and A Matrices

Every square matrix satisfies a unique polynomial, called the minimal polynomial. The minimal polynomial $m(\lambda)$ of a square matrix B is the polynomial of *lowest* degree for which $m(B) = 0$. Furthermore, $m(\lambda)$ divides every polynomial which is satisfied by B (Ref. 3). Therefore, $m(\lambda) \mid \phi(\lambda)$ where $\phi(\lambda)$ is the characteristic polynomial of B.

The length of the longest cycle of an FSR with linear logic feedback is related to the divisibility properties of $m(\lambda)$. Only when $\phi(\lambda) = m(\lambda)$, can $\phi(\lambda)$ be used to determine the length of all cycles (Ref. 1). To justify the use of $\phi(\lambda)$ or $\theta(\lambda)$ in determining the longest cycle length of FSRs associated with the T and A matrices, it must be shown that their characteristic and minimal polynomials are equal.

For any $n \times n$ matrix B, there exist elementary polynomial matrices $P(\lambda)$ and $Q(\lambda)$, such that

$$[P(\lambda)]\,[B-\lambda I]\,[Q(\lambda)] = \begin{bmatrix} d_1(\lambda) & 0 & \cdots & 0 \\ 0 & d_2(\lambda) & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & d_n(\lambda) \end{bmatrix} \tag{11}$$

where $d_1(\lambda), d_2(\lambda), \ldots, d_n(\lambda)$ are monic polynomials (see Ref. 6). The matrix $[B-\lambda I]$ satisfies (i.e., is a root of)

$$D(\lambda) = d_1(\lambda)\,d_2(\lambda), \ldots, d_n(\lambda) \tag{12}$$

in which $d_i(\lambda) \mid d_{i+1}(\lambda)$ for $i = 1, \ldots, n-1$. The diagonal matrix (Eq. 11) is the *Smith canonical* form of B and $d_i(\lambda)$ for all i is a *similarity invariant* of B. The minimal polynomial of B is $d_n(\lambda)$. The characteristic polynomial of B is $D(\lambda)$. When $D(\lambda) = d_n(\lambda)$, B is said to be nonderogatory.

The *Smith canonical* form can be derived from $[B-\lambda I]$ without explicitly determining $P(\lambda)$ and $\phi(\lambda)$. The *Smith canonical* form is derived as follows for the T and A matrices.

a. The T matrix. Given the 4×4 $[T-\lambda I]$ matrix,

$$\begin{bmatrix} \lambda+C_3 & C_2 & C_1 & 1 \\ 1 & \lambda & 0 & 0 \\ 0 & 1 & \lambda & 0 \\ 0 & 0 & 1 & \lambda \end{bmatrix} \tag{13}$$

Let the elementary transformations induced by $P(\lambda)$ or $Q(\lambda)$ be denoted as follows:

C_{ij} is the interchange of columns i and j

$C_{ij}(k)$ is the replacement of column i by column j plus k times column j

r_{ij}, $r_{ij}(k)$ are corresponding row operations

Note that all arithmetic operations are reduced modulo 2. The sequence of elementary operations

$$
\left.
\begin{array}{l}
(1)\ C_{21}(\lambda) \\
(2)\ r_{12}(\lambda + C_3) \\
(3)\ C_{32}(\lambda) \\
(4)\ r_{13}(\lambda^2 + C_3\lambda + C_2) \\
(5)\ C_{43}(\lambda) \\
(6)\ r_{14}(\lambda^3 + C_3\lambda^2 + C_2\lambda + C_1) \\
(7)\ r_{12} \\
(8)\ r_{23} \\
(9)\ r_{34}
\end{array}
\right\} \tag{14}
$$

reduces (13) to the Smith form

$$
\begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & \phi(\lambda)
\end{bmatrix} \tag{15}
$$

where $D(\lambda) = \phi(\lambda) = m(\lambda) = \lambda^4 + C_3\lambda^3 + C_2\lambda^2 + C_1\lambda + 1$.

This procedure is readily extended to any $r \times r$ T matrix as shown in Eq. (3) of Section 2.

b. The A matrix. Given the 5×5 $[A - \lambda I]$ matrix,

$$
\begin{bmatrix}
\lambda + C_3 & C_2 & C_1 & 1 & 1 \\
1 & \lambda & 0 & 0 & 0 \\
0 & 1 & \lambda & 0 & 0 \\
0 & 0 & 1 & \lambda & 0 \\
0 & 0 & 0 & 0 & \lambda + 1
\end{bmatrix} \tag{16}
$$

The sequence of elementary transformations from 1 through 6 as shown in (14) results in

$$
\begin{bmatrix}
0 & 0 & 0 & \phi(\lambda) & 1 \\
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & \lambda + 1
\end{bmatrix} \tag{17}
$$

and continuing with

$$
\begin{array}{l}
(7)\ C_{45}[\phi(\lambda)] \\
(8)\ r_{51}(\lambda + 1) \\
(9)\ C_{45} \\
(10)\ C_{34} \\
(11)\ C_{23} \\
(12)\ C_{12}
\end{array}
$$

reduces the matrix of (17) to

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & (\lambda + 1\phi(\lambda)
\end{bmatrix}
$$

4. Feedback Configuration for Near-Maximal Linear FSRs

a. Derivation of a characteristic polynomial for a cycle length of $2^r - 2$. Given the characteristic polynomial $g(\lambda)$ of degree r associated with a maximal-length r-stage linear FSR, then

$$\theta(\lambda) = (\lambda + 1)^2 g(\lambda)$$

is the characteristic polynomial of an $(r+2)$-stage linear FSR with a major cycle length of

$$2(2^r - 1) \text{ or } 2^{r+1} - 2$$

Since complementation of the feedback has the effect of introducing a factor of $\lambda + 1$ in the characteristic polynomial, a cycle length of $2^{r+1} - 2$ can be realized with an $(r+1)$-stage FSR, where

$$\phi(\lambda)^* = (\lambda + 1)\, g(\lambda)$$

For many values of r, a $g(\lambda)$ of degree r can be found such that $\phi(\lambda)^*$ is a tetranomial.

EXAMPLE 1:

$$g(\lambda) = \lambda^7 + \lambda^5 + \lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1$$

$$\phi(\lambda)^* = (\lambda + 1)\, g(\lambda) = \lambda^8 + \lambda^7 + \lambda^6 + 1 \tag{18}$$

or

$$\left.\begin{aligned} a_n &= 1 \oplus a_{n-1} \oplus a_{n-2} \oplus a_{n-8} \\ a_n &= a_{n-1} \oplus a_{n-2} \oplus a'_{n-8} \end{aligned}\right\} \quad (19)$$

The characteristic polynomial (Eq. 18), or equivalently, the linear recurrence relationship (Eq. 19), characterizes a major cycle length of 254 (and a minor cycle length of 2) of an eight-stage linear FSR.

The binary coefficients (1 0 1 1 1 1 1 1 in Example 1) may be determined from Ref. 5 for every maximal-length feedback configuration. When a $g(\lambda)$ is selected such that the binary sequence of coefficients starts and ends with a run of *ones* separated by a run of *zeros*,

$$\phi(\lambda)^* = (\lambda + 1)\, g(\lambda)$$

results in a tetranomial.

In Example 1, $(\lambda + 1)\, g(\lambda)$ can be determined from

$$g(\lambda) + \lambda g(\lambda)$$

as follows:

$$\begin{array}{lr} \;\;1\,0\,1\,1\,1\,1\,1\,1 & \lambda g(\lambda) \\ \,1\,0\,1\,1\,1\,1\,1\,1 & g(\lambda) \\ \hline 1\,1\,1\,0\,0\,0\,0\,0\,1 & (\lambda+1)\, g(\lambda) \end{array}$$

Table 1. Linear feedback configurations for FSR cycle lengths of $2^s - 2$ and 2

s	i	j	$2^s - 2$
4	1	2	14
5	1	3	30
6	1	2	62
7	1	5	126
8	1	2	254
9	2	6	510
10	2	3	1022
11	1	3	2046
12	2	7	4094
13	–	–	—
14	1	2	16328
15	3	5	32766
16	1	2	65534
17	1	11	131070
18	1	12	262142
19	1	7	524286
20	1	14	1048574

As shown in Table 1, there is an s-stage linear three-tap FSR with a major cycle length of $2^s - 2$ for every value of s from 4 through 20. The only exception is for an s of 13.

Where possible, it is desirable to have the stage storing a_{n-1} connected to the feedback. This allows a simplification in the implementation of the feedback when using RS flip-flops as memory elements. If the leading run of *ones* in the binary coefficient of $g(\lambda)$ contains a single *one* as in Example 1, the feedback function for $(\lambda + 1)\, g(\lambda)$ will be

$$a_{n-1} \oplus a_{n-j} \oplus a'_{n-s}$$

Each feedback configuration tabulated in Table 1 has a minor cycle of length 2. The states of the minor cycles are:

S even	S odd
0 1 0 1 · · · 0 1	0 1 0 1 · · · 0 1 0
1 0 1 0 · · · 1 0	1 0 1 0 · · · 1 0 1

b. Derivation of a characteristic polynomial for a cycle length of $2^s - 4$. The characteristic polynomial

$$\theta(\lambda) = (\lambda + 1)^3\, g(\lambda)$$

where $g(\lambda)$ is of degree r and maximal is the characteristic polynomial of an $(r+3)$-stage linear FSR with a major cycle length of

$$4(2^r - 1) \text{ or } 2^{r+2} - 4$$

A major cycle length of $2^{r+2} - 4$ can be realized with an $(r + 2)$-stage linear FSR. By complementing the feedback, a factor of $\lambda + 1$ is introduced. Thus,

$$\phi(\lambda)^* = (\lambda + 1)^2\, g(\lambda) = (\lambda^2 + 1)\, g(\lambda)$$

characterizes a linear FSR with a major cycle length of $2^{r+2} - 4$ and a minor cycle length of 4.

EXAMPLE 2:

$$g(\lambda) = \lambda^8 + \lambda^7 + \lambda^6 + \lambda^5 + \lambda^4 + \lambda^2 + 1$$

$$\phi(\lambda)^* = (\lambda^2 + 1)\, g(\lambda) = \lambda^{10} + \lambda^9 + \lambda^5 + 1 \quad (20)$$

or

$$\left.\begin{aligned} a_n &= 1 \oplus a_{n-1} \oplus a_{n-5} \oplus a_{n-10} \\ a_n &= a_{n-1} \oplus a_{n-5} \oplus a'_{n-10} \end{aligned}\right\} \qquad (21)$$

The characteristic polynomial (Eq. 20), or equivalently, the linear recurrence relationship (Eq. 21), characterizes a major cycle length of 1020 (and a minor cycle length of 4) of 10-stage linear FSR.

When a $g(\lambda)$ is selected such that the binary sequence of coefficients either starts with a run of *ones* and ends with alternating *zeros* and *ones* (i.e., 1 1 0 1 · · · 0 1), or starts and ends with alternatiing subsequences separated by a run of *zeros* or *ones*, $\phi(\lambda)^* = (\lambda + 1)^2 g(\lambda)$ results in a tetranomial. A $g(\lambda)$ of the first form yields a feedback configuration in which a_{n-1} is fed back.

In Example 2, $(\lambda^2 + 1) g(\lambda)$ can be determined from $g(\lambda) + \lambda^2 g(\lambda)$ as follows:

$$\begin{array}{r r} 1\,1\,1\,1\,1\,0\,1\,0\,1 & \lambda^2 g(\lambda) \\ 1\,1\,1\,1\,1\,0\,1\,0\,1 & g(\lambda) \\ \hline 1\,1\,0\,0\,0\,1\,0\,0\,0\,0\,1 & (\lambda^2 + 1) g(\lambda) \end{array}$$

Linear s-stage FSRs with a three-tap feedback configuration and a major cycle length of $2^s - 4$ are tabulated in Table 2. Values of s from 4 through 21 are included, with the exception of 6, 8, and 14 which do not exist with three feedback taps (i.e., which can be characterized with tetranomials).

Each feedback configuration tabulated in Table 2 has a minor cycle of length 4. The states of the minor cycle are:

0 0 1 1 0 0 1 1 · · · · 0 0 1 1 · · ·
1 0 0 1 1 0 0 1 · · · · 1 0 0 1 · · ·
1 1 0 0 1 1 0 0 · · · · 1 1 0 0 · · ·
0 1 1 0 0 1 1 0 · · · · 0 1 1 0 · · ·

Table 2. Linear feedback configurations for FSR cycle lengths of $2^s - 4$ and 4

s	i	j	$2^s - 2$
4	1	3	12
5	1	2	28
6	–	–	—
7	1	4	124
8	–	–	—
9	1	2	508
10	1	5	1020
11	1	4	2044
12	1	3	4092
13	1	2	8188
14	–	–	—
15	1	12	32764
16	1	7	65532
17	1	14	131068
18	5	9	262140
19	7	10	524284
20	5	7	1048572
21	1	6	2097148

c. Implementation of near-maximal linear FSRs. As shown in Tables 1 and 2, a near-maximal cycle length can be realized with a feedback function of the form

$$a_{n-i} \oplus a_{n-j} \oplus a'_{n-s}$$

for values of s from 4 through 21.

Substituting q_i for a_{n-i}, the next state of the leftmost memory element may be expressed as

$$Q_1 = q_i \oplus q_j \oplus q'_s \qquad (22)$$

Given RS flip-flops with the characteristic equation

$$Q = S' + Rq$$

where

$$R'S' = 0$$

the minimized R_1 and S_1 inputs for the flip-flops whose next state is Q_1 are:

(1) $i = 1$

$$R_1 = (q_1 q'_j q'_s + q_1 q_j q_s)'$$

$$S_1 = (q'_1 q'_j q'_s + q'_1 q_j q_s)'$$

(2) $i \neq 1$

$$R_1 = q'_i q_j q_s + q_i q'_j q_s + q_i q_j q'_s + q'_i q'_j q'_s$$

$$S_1 = R'_1$$

Thus, the cost of the feedback network is four NAND gates when $i = 1$ and five NAND gates when $i \neq 1$.

Provision for common collector operation (i.e., NAND-AND) is assumed.

When a maximal-length cycle of $2^r - 1$ cannot be realized with r stages, a near-maximal length of $2^r - 2$ or $2^r - 4$ may be realized with r stages and as few as four NAND gates which comprise the feedback network. (Two-tap feedback networks for maximal-length linear FSRs require two NAND gates when q_1 is fed back, or three NAND gates otherwise.)

For example, there is no 12-stage, two-tap feedback configuration that yields a maximal length of 4095 (see Ref. 2). However, the near-maximal length of 4092 can be realized with 12 memory elements and four NAND gates (see Table 2).

References

1. Elspas, B., "The Theory of Autonomous Linear Sequential Networks," *IRE Transactions on Circuit Theory*, Vol. CT-6, pp. 45–60, March 1959.
2. Golomb, S. W., Welch, L. R., and Hales, A., *On the Factorization of Trinomials Over GF(2)*. Memorandum 20-189, Jet Propulsion Laboratory, Pasadena, Calif., July 1959.
3. Birkhoff, G., and MacLane, S., *A Survey of Modern Algebra*, The MacMillan Company, New York, 1941.
4. Golomb, S. W., *Sequences With Randomness Properties*, Engineering Report 6193, The Martin Company, Engineering Laboratory, Baltimore, Md., June 14, 1955.
5. Marsh, R. W., *Table of Irreducible Polynomials Over GF(2) Through Degree 19*, OTS:PB-161,693, U. S. Department of Commerce, Office of Technical Services, Washington, D. C., October 24, 1957.
6. Albert, A. A., *Fundamental Concepts of Higher Algebra*, University of Chicago Press, Chicago, Ill., 1956.